RESULT LIST
1 result found in the Worldwide database for:
JP2003047065 (priority or application number or publication number)
(Results are sorted by date of upload in database)

1 TERMINAL ENABLING TO APPLY DATA LEAKAGE PREVENTING OPERATION FROM OUTSIDE

Inventor: YOSHIKAWA MASAKI

Applicant: DAINIPPON PRINTING CO LTD

EC:

IPC: ***G06F12/14; G06F15/02; H04L9/32*** (+9)

Publication info: **JP2003047065** - 2003-02-14

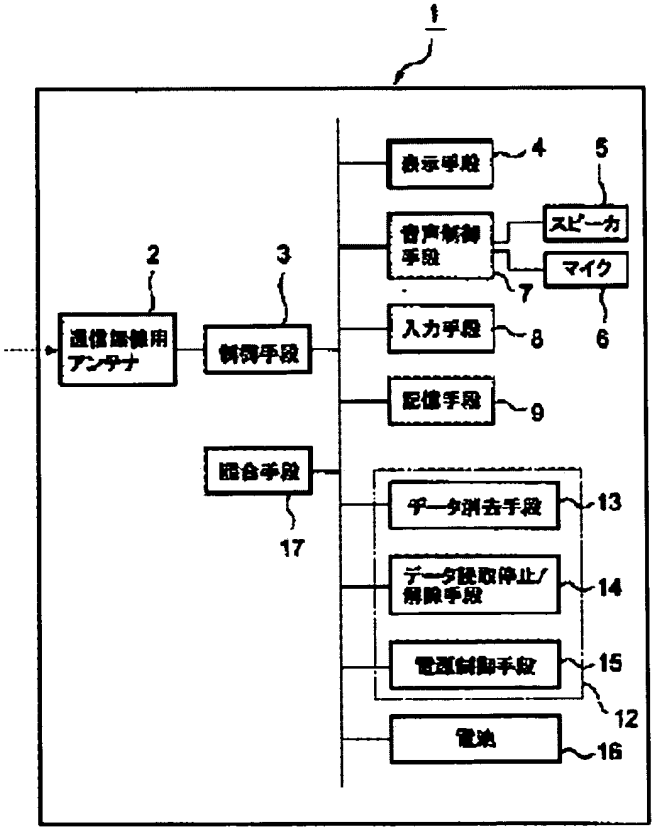
Data supplied from the ***esp@cenet*** database - Worldwide

TERMINAL ENABLING TO APPLY DATA LEAKAGE PREVENTING OPERATION FROM OUTSIDE

Patent number: JP2003047065
Publication date: 2003-02-14
Inventor: YOSHIKAWA MASAKI
Applicant: DAINIPPON PRINTING CO LTD
Classification:
- international: ***G06F12/14; G06F15/02; H04L9/32; H04Q7/38;*** **G06F12/14; G06F15/02; H04L9/32; H04Q7/38;** (IPC1-7): H04Q7/38; G06F12/14; G06F15/02; H04L9/32
- european:
Application number: JP20010234114 20010801
Priority number(s): JP20010234114 20010801

Abstract of **JP2003047065**

PROBLEM TO BE SOLVED: To provide a terminal enabling a data leakage preventing operation to be applied from outside, which can prevent data on a telephone number, etc., stored in the terminal from leaking to the third party even when the terminal of a mobile telephone set, etc., is passed to the third party by a theft, etc. SOLUTION: There are provided a storing means for storing a predetermined data and an ID password; a collating means for collating the received ID password with an ID password stored in the storing means when the ID password and a specific command were received from another terminal; and a data leakage preventing means for executing a data information leakage preventing process based on the specific command when the collated result of the collating means was coincident.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－47065
（P2003－47065A）
(43)公開日　平成15年２月14日(2003.2.14)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
H04Q	7/38		C06F	12/14	320D 5B017
G06F	12/14	320		15/02	335E 5B019
	15/02	335			360Z 5J104
		360	H04B	7/26	109R 5K067
H04L	9/32		H04L	9/00	673B

審査請求　未請求　請求項の数5　ＯＬ　（全６頁）

(21)出願番号　特願2001－234114(P2001－234114)

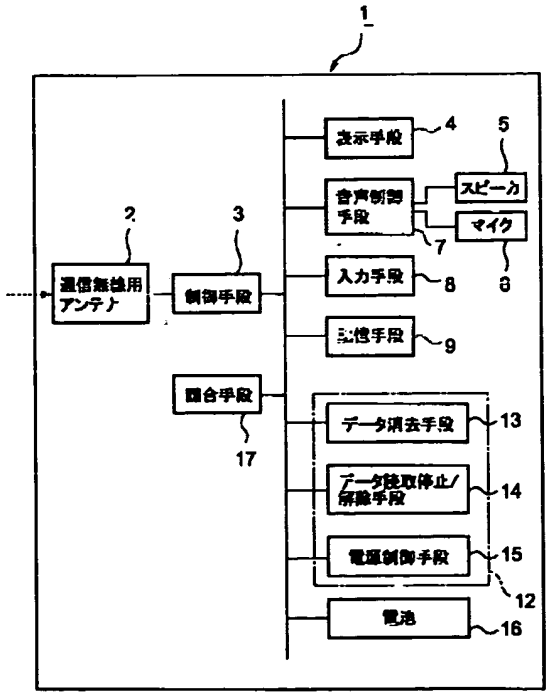
(22)出願日　平成13年８月１日(2001.8.1)

(71)出願人　000002897
大日本印刷株式会社
東京都新宿区市谷加賀町一丁目１番１号
(72)発明者　吉川　雅起
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内
(74)代理人　100111659
弁理士　金山　聡

最終頁に続く

(54)【発明の名称】　外部からデータ漏洩防止操作が可能な端末

(57)【要約】
【課題】　たとえ携帯電話機などの端末が盗難などで第三者に渡った場合でも、端末に記憶されている電話番号などのデータが第三者に漏れるのを防止することができる外部からデータ漏洩防止操作が可能な端末を提供する。
【解決手段】　所定のデータ及び照合用パスワードが記憶された記憶手段と、他の端末から照合用パスワードと特定のコマンドを受信した際に、受信した照合用パスワードと前記記憶手段に記憶されている照合用パスワードとを照合する照合手段と、前記照合手段の照合結果が一致した場合に、前記特定のコマンドに基づいたデータ情報漏洩防止処理を実行するデータ漏洩防止処理手段を備えていることを特徴とする。



【特許請求の範囲】
【請求項１】　所定のデータ及び照合用パスワードが記憶された記憶手段と、他の端末から照合用パスワードと特定のコマンドを受信した際に、受信した照合用パスワードと前記記憶手段に記憶されている照合用パスワードとを照合する照合手段と、前記照合手段の照合結果が一致した場合に、前記特定のコマンドに基づいたデータ情報漏洩防止処理を実行するデータ漏洩防止処理手段を備えていることを特徴とする外部からデータ漏洩防止操作が可能な端末。
【請求項２】　所定のデータが記憶された記憶手段と、公開鍵暗号方式を利用して、他の端末から電子署名を付加した特定のコマンドが受信された際に、前記電子署名を検証する電子署名検証手段と、公開鍵が登録された公開鍵登録手段と、前記電子署名検証手段で検証された場合に、前記特定のコマンドに基づいたデータ情報漏洩防止処理を実行するデータ漏洩防止処理手段を備えていることを特徴とする外部からデータ漏洩防止操作が可能な端末。
【請求項３】　前記データ漏洩防止処理手段が、前記特定のコマンドに対応して、前記記憶手段に記憶されているデータの消去処理を行なう消去手段である特徴とする請求項１又は請求項２に記載の外部からデータ漏洩防止操作が可能な端末。
【請求項４】　前記データ漏洩防止処理手段が、前記特定のコマンドに対応して、前記記憶手段に記憶されているデータの読み取りを一時的に停止、または停止状態を解除させる機能を有するデータ読取停止／解除手段である特徴とする請求項１記載又は請求項２に記載の外部からデータ漏洩防止操作が可能な端末。
【請求項５】　前記データ漏洩防止処理手段が、前記特定のコマンドに対応して、前記端末の電源を一時的にＯＦＦ状態とし、又はＯＦＦ状態からＯＮ状態に戻す機能を有する電源制御手段である特徴とする請求項１又は請求項２に記載の外部からデータ漏洩防止操作が可能な端末。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、携帯電話機などの端末が盗難などにあったりして、第三者にその端末が渡った場合でも、端末に記憶されている電話番号などのデータが不正に漏洩されるのを防止することができる外部からデータ漏洩防止操作が可能な端末に関する。
【０００２】携帯電話機などの端末は、いつでもどこへでも持ち運んで使用することができて便利である反面、うっかりどこかに置き忘れて第三者に持っていかれたり、また簡単に盗難に会うなどの危険性も高い。その場合、携帯情報端末機などの端末に記憶されている電話番号などのデータが、本人が知らない間に第三者に漏れて悪用されるなどセキュリティー上の危険性があり問題である。
【０００３】
【発明が解決しようとする課題】本発明は、たとえ携帯電話機などの端末が盗難などで第三者に渡った場合でも、端末に記憶されている電話番号などのデータが第三者に漏れるのを防止することができる外部からデータ漏洩防止操作が可能な端末を提供する。
【０００４】
【課題を解決するための手段】本発明の外部からデータ漏洩防止操作が可能な端末は、所定のデータ及び照合用パスワードが記憶された記憶手段と、他の端末から照合用パスワードと特定のコマンドを受信した際に、受信した照合用パスワードと前記記憶手段に記憶されている照合用パスワードとを照合する照合手段と、前記照合手段の照合結果が一致した場合に、前記特定のコマンドに基づいたデータ情報漏洩防止処理を実行するデータ漏洩防止処理手段を備えていることを特徴とする。
【０００５】また、本発明の外部からデータ漏洩防止操作が可能な端末は、所定のデータが記憶された記憶手段と、公開鍵暗号方式を利用して、他の端末から電子署名を付加した特定のコマンドが受信された際に、前記電子署名を検証する電子署名検証手段と、公開鍵が登録された公開鍵登録手段と、前記電子署名検証手段で検証された場合に、前記特定のコマンドに基づいたデータ情報漏洩防止処理を実行するデータ漏洩防止処理手段を備えていることを特徴とする。
【０００６】更に、本発明は、前記データ漏洩防止処理手段が、前記特定のコマンドに対応して、前記記憶手段に記憶されているデータの消去処理を行なうデータ消去手段である特徴とする。また、本発明は、前記データ漏洩防止処理手段が、前記特定のコマンドに対応して、前記記憶手段に記憶されているデータの読み取りを一時的に停止、または停止状態を解除させる機能を有するデータ読取停止／解除手段である特徴とする。
【０００７】更に、本発明は、前記データ漏洩防止処理手段が、前記特定のコマンドに対応して、前記端末の電源を一時的にＯＦＦ状態とし、又はＯＦＦ状態からＯＮ状態に戻す機能を有する電源制御手段である特徴とする。
【０００８】
【発明の実施の形態】以下、本発明の実施の形態を図面に基づいて詳細に説明する。図１は、本発明の外部からデータ漏洩防止操作が可能な端末にかかる第１実施形態のシステムブロック図、図２は、本発明の第１実施形態の端末を用いて、外部からデータの漏洩防止の操作を行なう場合を説明する図、図３は、本発明の外部からデータ漏洩防止操作が可能な端末にかかる第２実施形態のシステムブロック図、図４は、本発明の第２実施形態の端末を用いて、外部からデータの漏洩防止の操作を行なう場合を説明する図である。

【0009】以下、本発明の第1実施形態に係る端末について説明する。ここでは、説明しやすいように端末として、携帯電話機を一例として以下説明する。

【0010】本発明の端末である携帯電話機1は、図1のシステムブロック図に示されているように、通信無線用アンテナ2、制御手段3、ディスプレイからなる表示手段4、スピーカ5及びマイク6の音声を制御する音声制御手段7、入力手段8、記憶手段9、データ漏洩防止手段12、電池16、照合手段17とを備えている。

【0011】記憶手段9には、予め照合用パスワードを記憶させておく。また、データ漏洩防止手段12としては、例えばデータ消去手段13、データ読取停止/解除手段14、電源制御手段15が備えられている。これらのデータ漏洩防止手段12は、必ずしも、上記のデータ消去手段13、データ読取停止/解除手段14、電源制御手段15の全てを備えていなくてもよく、これらの手段の中から少なくとも1つの手段を備えていればよいものである。

【0012】このデータ消去手段13は、記憶手段9に記憶された電話番号やメールなどの所定のデータを消去処理する機能を有するが、データ消去手段13がこれらの消去処理を行なうためには、予め定められた特定のコマンドを他の携帯電話機から受信することが前提となる。

【0013】また、データ読取停止/解除手段14は、記憶手段9に記憶されているデータの読み取りを一時的に停止、または停止状態を解除させる機能を有するものであり、データの読み取りを停止させる場合の処理とデータの読み取りを停止解除させる場合の処理を実行する際には、それぞれ予め定められた特定のコマンドが入力されることを条件とする。

【0014】これにより、他の携帯電話機から受信したコマンドに対応して、記憶手段9に記憶されているデータに対する読み取りの停止処理、または停止状態を解除する処理が行なわれる。停止状態を解除する処理は、例えば紛失した携帯電話機が戻ってきた場合に、再度携帯電話機の記憶手段9に記憶されているデータを使用できるようにするための機能である。

【0015】また、電源制御手段は、他の携帯電話機から受信したそれぞれの特定のコマンドに対応して、携帯電話機の電源を一時的にOFF状態とし、又は電源を一時的にOFF状態とした後は、店舗に持っていって特殊な処理をしないと再度電源ON状態に戻すことができない機能を有するものである。携帯電話機の電源を一時的にOFF状態とすることで、記憶手段9に記憶されたデータの読み取りができなくなり、データの漏洩が防止される。また、再度ON状態に戻す機能は、例えば紛失した携帯電話機が戻ってきた場合に、再度携帯電話機の使用ができるようにするための機能である。

【0016】照合手段17は、他の携帯電話機から受信した照合用パスワードと、利用者本人の携帯電話機の記憶手段9に記憶されている照合用パスワードとを照合するもので、照合手段17による照合結果が一致した場合にだけ、他の携帯電話機から受信したコマンドに対応した種々の処理が行なわれる。

【0017】次に、利用者本人の携帯電話機が盗難などで第三者に渡った場合の処理手順について説明する。利用者は、他の携帯電話機を使用して、利用者本人の携帯電話機に対して電話をかけるが、その際に、電話番号に続けて照合用パスワードとコマンドを入力する。そして、電話番号と照合用パスワードとコマンドを、他の携帯電話機から利用者本人の携帯電話機に対して送信する。

【0018】利用者本人の携帯電話機では、受信した照合用パスワードと、予め記憶手段9に記憶させておいた照合用パスワードを照合手段17で照合する。そして、この照合手段17での照合での結果が一致した場合、他の携帯電話機から利用者本人の携帯電話機に送信した特定のコマンドに基づき、データ漏洩防止手段12による記憶手段に記憶されたデータの漏洩防止の処理が行なわれる。

【0019】データ漏洩防止手段12によるデータの漏洩防止の処理としては、種々の手段による処理を平行して行なうことができる。例えば、データ漏洩防止手段12として、データ消去手段13、データ読取停止/解除手段14、電源制御手段15を備えた場合には、1種類の特定のコマンドに基づき、データ消去手段13で記憶手段に記憶されているデータの消去を行なう処理が実施され、また、データ読取停止/解除手段14で、記憶されているデータの読取停止処理が行なわれ、更に、電源制御手段15で携帯電話機の電源が切られるなどが行なわれる。

【0020】上記のデータ消去手段13、データ読取停止/解除手段14、電源制御手段15によるデータ漏洩防止手段12は、特定のコマンドとの関係により各手段の処理を選択することが可能になっている。例えば、データ漏洩防止手段12の各手段毎に異なるコマンドを定めておくことで、操作する手段と命令実行する機能を選択できるようにすることもできる。

【0021】次に、本発明の第2実施形態にかかる端末について説明する。図3には、本発明の第2実施形態にかかる端末である携帯電話機20のシステムブロック図が示されている。本発明の第2実施形態における携帯電話機20は、本発明の第1実施形態における携帯電話機1に備えている照合手段17を有していないが、その代わりにICカード10のメモリに記憶されたデータの読み取り又はメモリへのデータの書き込みを行なう読取書込手段11と、公開鍵登録手段18と、電子署名検証手段19とを有している。

【0022】また、第2実施形態における携帯電話機2

０に使用するＩＣカード１０には、公開鍵暗号方式を用いることが可能な暗号処理機能と秘密鍵が記憶された記憶手段とを有している。この暗号処理機能と秘密鍵により、携帯電話機２０で送信するコマンドに電子署名を付し、送信することができるようにしてある。

【００２３】第２実施形態では、他の携帯電話から利用者本人の携帯電話機２０に送信されるコマンドを公開鍵方式を利用して行なう場合を前提としている。携帯電話機２０に備えられた公開鍵登録手段１８と電子署名検証手段１９は、他の携帯電話機から送信され、携帯電話機２０で受信した電子署名を付したコマンドを、公開鍵登録手段１８に登録された公開鍵で復号した後、復号したコマンドと最初から暗号化されずに送信されてきたコマンドを照合して検証するためのものである。

【００２４】次に、利用者本人の携帯電話機が盗難などで第三者に渡った場合の処理手順について説明する。図４には、盗難などで第三者に渡った利用者本人の携帯電話機２０Ａに対して、利用者が、他の携帯電話機２０Ｂを使用して電話をかけた場合について示している。この場合、利用者は、ＩＣカードは紛失しないで所持しているものとする。

【００２５】利用者は、他の携帯電話機２０ＢにＩＣカード１０をセットし、携帯電話機２０Ｂの読取書込手段１１によりデータの読取り及び書込みを行なえる状態とした後、入力手段８からデータ漏洩防止手段１２の漏洩防止を図るために予め定められた特定のコマンドを入力する。

【００２６】入力手段８から入力されたこのコマンドは、ＩＣカード１０の暗号処理機能により、秘密鍵で暗号化されて電子署名が付される。そして、電子署名が付されたコマンドは、他の携帯電話機２０Ｂから利用者本人の携帯電話機２０Ａに対して、メール送信される。

【００２７】次に、電子署名が付されたコマンドのメールを受信した利用者本人の携帯電話機２０Ａでは、公開鍵登録手段１８に記憶されている公開鍵を使用して、電子署名検証手段１９により受信したデータの改ざんが行なわれていないかの検証が行なわれる。

【００２８】上記の電子署名検証手段１９による検証結果が一致した場合には、受信したコマンドに基づいたデータ漏洩防止手段１２であるデータ消去手段１３、データ読取停止／解除手段１４、電源制御手段１５の各手段による漏洩防止の処理が実行される。第２実施形態における携帯電話機２０では、公開鍵暗号方式を用いてデータ漏洩防止手段１２の実行に必要なコマンドの送受信が行なわれるので、利用者本人でなければ送信するコマンドに電子署名を付すことができないので、データのセキュリティーが保持できる。

【００２９】上記の実施形態では、携帯情報端末機として携帯電話機の場合について説明したが、携帯電話機に限定されるものではなく、その他様々な携帯情報端末機に適応することができるものである。

【００３０】

【発明の効果】以上説明したように、本発明の本発明の外部からデータ漏洩防止操作が可能な端末は、たとえ携帯電話機などの端末が盗難などで第三者に渡った場合でも、外部からこの端末に特定のコマンドを送信することで、端末の記憶手段に記憶されたデータの漏洩防止を図ることができるという効果がある。

【図面の簡単な説明】

【図１】本発明の外部からデータ漏洩防止操作が可能な端末にかかる第１実施形態のシステムブロック図である。

【図２】本発明の第１実施形態の端末を用いて、外部からデータの漏洩防止の操作を行なう場合を説明する図である。

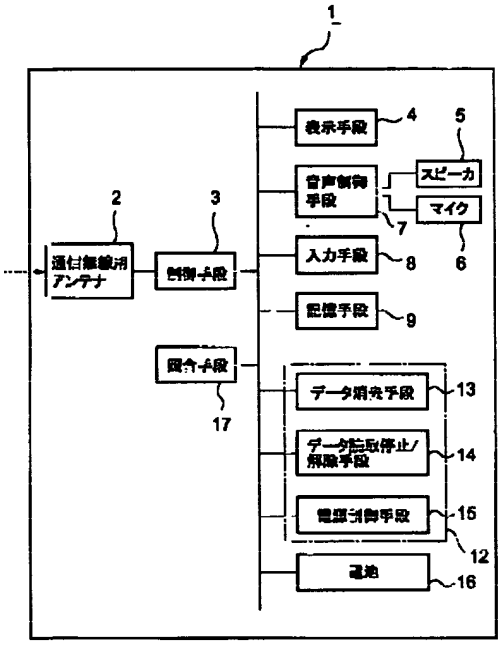
【図３】本発明の外部からデータ漏洩防止操作が可能な端末にかかる第２実施形態のシステムブロック図である。

【図４】、本発明の第２実施形態の端末を用いて、外部からデータの漏洩防止の操作を行なう場合を説明する図である。

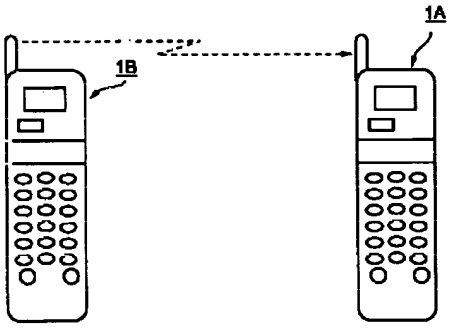
【符号の説明】

１，１Ａ，１Ｂ，２０，２０Ａ，２０Ｂ　携帯電話機
２　通信無線用アンテナ
３　制御手段
４　表示手段
５　スピーカ
６　マイク
７　音声制御手段
８　入力手段
９　記憶手段
１０　ＩＣカード
１１　読取書込手段
１２　データ漏洩防止手段
１３　データ消去手段
１４　データ読取停止／解除手段
１５　電源制御手段
１６　電池
１７　照合手段

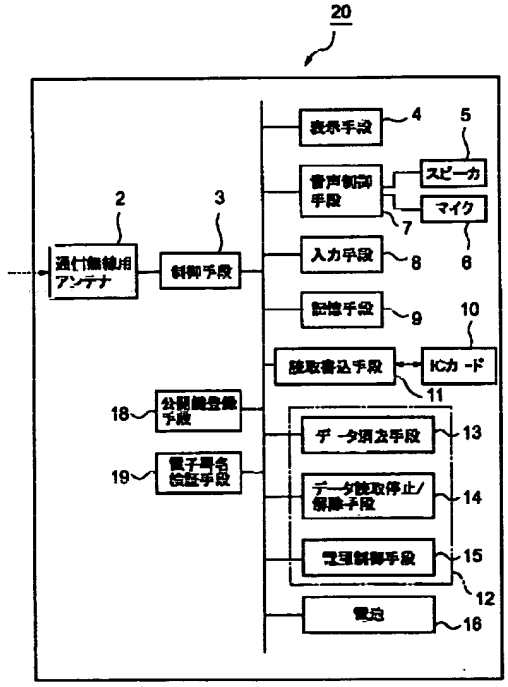
【図1】


1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
通信無線用アンテナ
制御手段
表示手段
音声制御手段
スピーカ
マイク
入力手段
記憶手段
ICカード
データ消去手段
データ読取停止/解除手段
電源制御手段
電池
公開鍵登録手段
電子署名検証手段

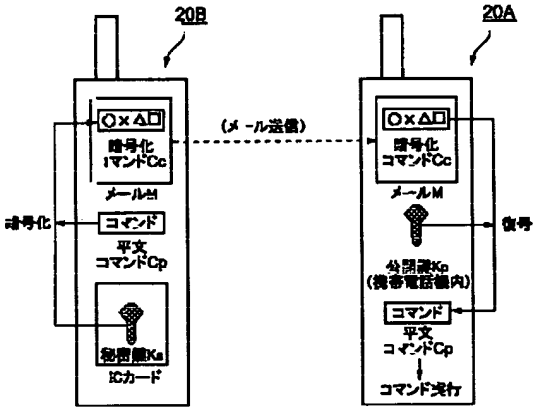
【図2】


1A
1B

【図3】


20
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
18
19
通信無線用アンテナ
制御手段
表示手段
音声制御手段
スピーカ
マイク
入力手段
記憶手段
読取書込手段
ICカード
公開鍵登録手段
電子署名検証手段
データ消去手段
データ読取停止/解除手段
電源制御手段
電池

【図4】


20B
20A
(メール送信)
暗号化コマンドCc
メールM
暗号化
コマンド
平文コマンドCp
秘密鍵Ks
ICカード
公開鍵Kp
(携帯電話機内)
復号
コマンド実行

フロントページの続き

Fターム(参考) 5B017 AA07 BA05 BA08 CA14
5B019 GA10 HF10
5J104 AA07 AA09 KA02 KA05 LA06
NA02 NA05 PA02
5K067 AA30 AA32 BB04 DD27 HH22
HH23 HH24 HH36